UIC John Marshall Journal of Information Technology & Privacy Law

Volume 22
Issue 2 *Journal of Computer & Information Law - Winter 2004*

Article 4

Winter 2004

The Global Rise of a Duty to Disclose Information Security Breaches, 22 J. Marshall J. Computer & Info. L. 457 (2004)

Ethan Preston

Paul Turner

THE GLOBAL RISE OF A DUTY TO DISCLOSE INFORMATION SECURITY BREACHES

ETHAN PRESTON†
AND PAUL TURNER††

On July 1, 2003, California's Security Breach Information Act took effect.[1] Section 1798.82 requires computer database operators to disclose security breaches that involve data containing personal information to both the subjects of the data and to the owners of personal data. Critics of the law have split much ink over the potential problems of litigation and negative exposure posed by Section 1798.82.[2] While this commen-

† B.A., University of Texas at Austin, 1998. J.D., Georgetown University Law Center, 2001. Mr. Preston is an associate at Aronberg, Goldgehn, Davis & Garmisa.

†† B.A., Harvard College, 1975. J.D., Harvard Law School, 1978. Mr. Turner is a partner at McCullough, Campbell & Lane.

1. Cal. Civ. Code § 1798.82 (West 2003) (available at <http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84>).

2. *See e.g.* Cheryl A. Falvey et. al., *Disclosure of Security Breaches Required by New California Privacy Legislation*, Metro. Corp. Couns. 5 (Aug. 2003) (stating that "many predict that the disclosure obligation will result in massive class action suits for companies victimized by security breaches"); Mathias Thurman, *IT Security Confronts New Legal Liabilities; Upcoming legislation and changing threats prompt our cautious security manager to double-check the corporate liability policy*, Computerworld 38 (June 23, 2003); Nick Akerman & Gabrielle Wirth, *New Identity Theft Law*, 25 Natl. L.J. P18 (June 16, 2003); Donna Howell, *California Law Raises Bar For Data Security*, Investor's Bus. Daily A05 (June 6, 2003); George V. Hulme, *California's New Rules Of Disclosure - State law will force companies nationwide to make security breaches public*, Information Week 26 (June 23, 2003) (stating that "[a] California law that takes effect July 1 will force companies inside and outside the state to do what they historically have been loath to do: disclose embarrassing information-security breaches"); Mary J. Hildebrand & Jacqueline Klosek, *New California Data Security Law to Have Broad Reach*, Mondaq Bus. Briefing (May 14, 2003); Jerald M. Savin, *Identity theft bill brings nightmare for businesses*, L.A. Bus. J. 52 (May 12, 2003) (stating that "[t]his bill is a leap forward in the fight against identity theft. It is also a potential nightmare for computer security and a business public image"); Katie Kuehner-Hebert, *A New Law on Data Security Could Produce PR Headaches*, Am. Banker 1 (Apr. 8, 2003) (noting that "[i]ndividual bankers contacted for this story did not want to comment on the state's new law, but privately they said they are concerned that once these notices start arriving, customers may panic and yank deposits. The law could become a public relations nightmare for an industry based on trust"); Melissa Solomon, *Bank Allies*

tary reflects apprehension about the impending duty to disclose security breaches under section 1798.82, a more thorough examination shows much broader duties to disclose such breaches are already in place. In the final analysis, section 1798.82 emerges as neither groundbreaking nor as outlandish as much of the commentary suggests. Rather, it codifies duties that are already present in many of the relationships between data subjects and data collectors.

At the outset, commentary has largely overlooked Article 4 of the European Union Telecommunications[3] and Electronic Communications Privacy Directives,[4] and (as an example of European implementation) British implementation.[5] Article 4, in both the old Telecommunications Privacy Directive and the new Electronic Communications Privacy Directive, expressly requires the disclosure of security risks to consumers, in much the same way that section 1798.82 does. Despite this similarity, these legislative initiatives have many important differences. Section I describes and compares these two laws.

While Section I adds an overlooked element to the description of the duty to disclose information security breaches, it falls short of giving the complete outlines of that duty. The California statute, the European directive and its British implementing legislation merely supplement a wider world of privacy laws by requiring entities holding personal data to inform data subjects when their data has been disclosed in an unauthorized fashion (including by a computer intrusion). The wider world of privacy law tends not to prohibit the disclosure of information outright. Rather, it tends to require entities to disclose, when they collect data from data subjects, how it will be maintained and with whom it will be shared, and to punish entities that do not live up to their representations. Although entities' representations of their information practices may occur in the context of complying with sophisticated regulations, the representations may still be the basis of liability under the common law. Negligent and fraudulent representations about data disclosure can trigger older, common law causes of action. Section II explains how various privacy regulations dovetail with these common law doctrines to generate a very broad duty to disclose information security breaches.

Say California Hacking Law Goes Too Far, 16 Bank Tech. News 37 (Mar. 2003); Elaine M. Laflamme, *Know the Liabilities of Data Collection! And Understand Issues Well Before Putting Better, Faster, Cheaper Technology to Work*, 229 N.Y. L.J. 6 (Feb. 3, 2003).

3. Directive 97/66/EC (Dec. 15, 1997) (concerning the processing of personal data and the protection of privacy in the telecommunications sector) (available at <http://europa.eu.int/eur-lex/en/search/ search_lif.html>).

4. Directive 2002/58/EC (July 12, 2002) (concerning the processing of personal data and the protection of privacy in the electronic communications sector) (available at <http://europa.eu.int/eur-lex/en/search/search_lif.html>).

5. Telecommunications (Data Protection and Privacy) Regulations (1999) SI 1999/2093 (available at <http://www.legislation.hmso.gov.uk/si/si1999/19992093.htm>).

I. LEGISLATION EXPRESSLY REQUIRING DISCLOSURE OF COMPUTER SECURITY BREACHES

On April 5, 2002, computer intruders successfully gained unauthorized access to state employees' sensitive financial and personal information stored at the Stephen P. Teale Data Center in Sacramento, California.[6] The intrusion affected approximately 265,000 California state employees, but, although the incident was reportedly discovered as of May 7, 2002, the affected state employees were not notified until May 21, 2002.[7] Between the time the hackers accessed the database and the disclosure of the attack, attempts were made to access one state worker's bank account and to change the address for another worker's credit card account.[8] These events, and the Data Center's subsequent failure to inform the state employees at risk, prompted the amendments to section 1798.82. Section 1798.82's legislative history also discusses an incident where Bank One failed to disclose to its customers that a former employee sold hundreds of financial records to an identity theft ring.[9]

Information security breaches are increasingly widespread. In one of the most notorious incidents, a computer criminal broke into CD Universe's database and posted customers' credit card numbers on the Internet after the company refused to fulfill the criminal's $100,000 extortion demand.[10] Indeed, the problems described in the legislative history are endemic to the computer and information technology industry. The Computer Security Institute 2003 Computer Crime and Security Survey surveyed 530 information security professionals: thirty-six percent of the 490 respondents experienced some form of system penetration breach in the past year, while twenty-one percent had dealt with theft of proprietary information.[11] Despite the widespread penetration of databases, only thirty percent of respondents reported these incidents to law enforcement and twenty-one percent reported to legal counsel, while *fifty percent did not report these incidents at all.*[12] Underreporting computer security incidents is not limited to the U.S. – one European study estimates 30,000 to 40,000 occurred in one European nation, while

6. Cal. Sen. Assembly Comm. on Bus. and Professions, *Hearing on SB 1386* 2001-2002 Leg. 2d Sess. 5 (Aug. 6, 2002) (available at <http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_13511400/sb_ 1386_cfa_20020804_191651_asm_comm.html>).

7. *Id.* at 4.

8. *Id.*

9. *Id.*

10. Alan Charles Raul, Frank R. Volpe & Gabriel S. Meyer, *Liability for Computer Glitches and Online Security Lapses*, 6 BNA Elec. Com. L. Rep. 849 (Aug. 31, 2001) (available at <http://www.sidley.com/cyberlaw/features/liability.asp>); *see also* Katie Hafner & John Biggs, *In Net Attacks, Defining the Right to Know*, N.Y. Times G1 (Jan. 30, 2003).

11. Robert Richardson, Computer Security Institute, *2003 CSI/FBI Computer Crime and Security Survey* 4, <http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf> (2003).

12. *Id.* at 18.

only 105 official complaints were made.[13]

The resulting amendments to section 1798.82 now require businesses (and other entities that collect personal information and operate computer databases) to disclose security risks and security breaches to their customers.[14] As the legislative history for section 1798.82 notes, database operators have strong motivations to suppress computer security breaches.

> All too often events of this sort go completely unreported. How can this be? The embarrassment of disclosure that a company or agency was "hacked," or the fear of lost business based upon shoddy information security practices being disclosed overrides the need to inform the affected persons. In other instances, credit card issuers, telephone companies and internet service providers, along with state and local officials "handle" the access of consumer's personal and financial information by unauthorized persons internally, often absorbing the losses caused by fraud as a matter of "customer service" without ever informing the customer of the unauthorized use of his/her account. Customers need to know when unauthorized activity occurs on their accounts, or when unauthorized persons have access to sensitive information, in order to take appropriate steps to protect their financial health.[15]

Requiring businesses to disclose information security violations provides operators with a market incentive to ensure that their security is adequate. While potential liability and litigation costs will motivate data collectors to secure their data, market discipline for poor security (and market rewards for good security) may provide even stronger incentives to secure their data. Customers will be reluctant to transact with businesses that fail to adequately secure their databases. Further, when consumers have notice of unauthorized access to their personal information, they can take steps to mitigate the potential harm by informing credit reporting agencies and responding to fraudulent attempts to exploit their good names. Commercial clients that store valuable intellectual property with the database operator may be able to mitigate the harm of having their property released to computer criminals with sufficient notice. Disclosure permits all customers to identify and avoid businesses that do not take their computer security seriously or are unable to do so.

---

13. The European Commission, *Proposal for a Council Framework Decision on attacks against information systems,* COM (2002) 173 final at 5 (available at <http://europa.eu.int/eur-lex/en/ com/pdf/2002/com2002_0173en01.pdf>).

14. Cal. Civ. Code § 1798.82 (West 2003).

15. Cal. Sen. Assembly Comm. on Bus. and Professions, *Hearing on SB 1386* 2001-2002 Leg. 2d Sess. 5 (Aug. 6 2002) (available at <http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_cfa_20020804_191651_asm_comm.html>).

A. California Civil Code Section 1798.82

The California legislature specifically drafted section 1798.82 to address identity theft concerns. It requires disclosure in the event there are reasonable grounds to believe that unauthorized intruders have breached security and accessed data containing personal information. However, the disclosure requirement has specific limits on who is protected, what kinds of data are protected against which kind of intrusions, and when disclosures must be made. Section 1798.82 also specifies how adequate disclosure can be made. As a consequence, there are a number of significant conditions and qualifications to section 1798.82's disclosure requirement.

1. *What Data Are Protected*

Personal information is defined as an unencrypted combination of data including a person's first name (or first initial) and last name, along with

- a Social Security number;
- a Driver's license number;
- California Identification Card number; or
- an account number, credit or debit card number, along with any required security code, access code, or password that would permit access to an individual's financial account.[16]

However, personal information does not include any information lawfully available to the general public from any government records.[17]

A breach of security is defined as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business."[18] However, acquisition of personal information by a database operator employee for the operator's purposes, and in good faith, is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.[19]

2. *When Disclosure to Data Subjects Is Required*

Section 1798.82 requires any person conducting business in California to disclose any breach of security "following discovery or notification of the breach in the security of computerized personal data with personal information to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an

16. Cal. Civ. Code § 1798.82(e) (West 2003).
17. *Id.* at § 1798.82(f).
18. *Id.* at § 1798.82(e).
19. *Id.*

unauthorized person."[20] Computer database operators must disclose the security breach "in the most expedient time possible and without unreasonable delay."[21] There are two exceptions: database operators may delay disclosure to the extent necessary to determine the scope of the breach and restore the reasonable integrity of the data system, and "consistent with the legitimate needs" of a law enforcement agency in a criminal investigation.[22]

3. *When Disclosure Is Required to Data Owners*

In addition, when database operators store computerized data they do not own, they also have a duty to disclose unauthorized access of data (containing personal information) to the data's owner or licensee "immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[23] Disclosure to data owners is much broader than to data subjects. Section 1798.82(b) does not explicitly restrict the obligation to disclose security breaches by the geographical location of either the database owner or the data subjects or by whether the data were encrypted or not (Presumably, then, data owners could enforce section 1798.82 to the limits of California's personal jurisdiction). In addition, there are no grounds for delaying disclosure: in other words, disclosure is to be made immediately.

4. *Disclosure Requirements*

Section 1798.82 provides specific requirements for notice of security breaches. Notice must be in written form or an electronic form that satisfies the requirements of 15 U.S.C. § 7001.[24] However, if the operator demonstrates that

- the cost of providing notice would exceed $250,000;
- that the affected class of persons to be notified exceeds 500,000 individuals; or
- that the operator does not have sufficient information to contact the affected individuals, the operator may use substitute notice.[25]

Substitute notice includes e-mail (when the e-mail address is available), conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one, and notification to a major statewide media outlet.[26] However, an operator with an informa-

20. Cal. Civ. Code § 1798.82(a).
21. *Id.*
22. *Id.* at § 1798.82(a), (c).
23. *Id.* at § 1798.82(b).
24. *Id.* at § 1798.82(g)(1), (2).
25. Cal. Civ. Code § 1798.82(g)(3).
26. *Id.*

tion security policy for personal information that includes its own notification procedures that otherwise adheres to the timing requirements of this part is deemed to have complied with section 1798.82 (provided it actually complies with those notification procedures).[27]

5. *Penalties*

Businesses must make reasonable efforts to destroy those customer records within their custody that no longer need "to be retained by the business."[28] California law provides for injunctions against the failure to destroy personal information or to disclose security breaches; and customers that provided personal information have a right of action for any damages.[29] Any waiver of rights under sections 1798.82 is contrary to public policy, void and unenforceable.[30]

B. The European Telecommunication and Electronic Communications Privacy Directives and the English Telecommunications (Data Protection and Privacy) Regulations 1999

The EU legislation relevant to the disclosure of computer security breaches is an organic development of previous EU privacy legislation. The security breach disclosure obligations in the contemporary Electronic Privacy Directive are best described by tracing their development from the provisions of the older EU Privacy Directive and through the intervening Telecommunications Privacy Directive.

1. *The EU Data Protection Directive and the British Implementation*

The EU Data Protection Directive regulates the processing and disclosure of personal data.[31] Moreover, it provided data subjects with extensive rights to information about the data collected on them, rights to access the data and rights to object to processing of the subject's personal data.[32] As part of a comprehensive regulation of personal information processing, Article 17 of the Data Protection Directive sets security requirements for processing personal data, requiring the party responsible for the data to:

---

27. *Id.* at § 1798.82(h).

28. *Id.* at §§ 1798.80(c), 1798.83 (West 2003).

29. *Id.* at §§ 1798.80(c), 1798.84 (West 2003).

30. Cal. Civ. Code § 1798.83.

31. Directive 95/46/EC arts. 6-9 (Oct. 24, 1995) (describing the protection of individuals with regard to the processing of personal data and on the free movement of such data) (available at <http://europa.eu.int/eur-lex/en/search/search_lif.html>).

32. Directive 95/46/EC arts. 10-12, 14 (1995).

> implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.[33]

Moreover, the data protection directive requires that "any person who has suffered damage" as a result of improper processing be able to receive compensation from the party responsible for the data.[34] The United Kingdom implemented the data protection directive through the *Data Protection Act 1998*,[35] which promulgated data subjects' rights[36] and data processors' notification obligations.[37]

2. *The EU Telecommunications Privacy Directive and the British Implementation*

The Telecommunications Privacy Directive[38] adapted and translated the general rules of data protection directive into specific rules for the telecommunications sector.[39] The relevant portions of the Telecommunications Directive applied to broadly defined publicly available telecommunications service providers[40] and their subscribers.[41] The Telecommunications Privacy Directive required that telecommunications service providers "take appropriate technical and organisational measures to safeguard the security of [their] services. . . having regard to the state of the art and the cost of implementation. These measures shall

---

33. Directive 95/46/EC art. 17(1) (1995).

34. Directive 95/46/EC art. 23 (1995).

35. Data Protection Act 1998, ch. 29 (available at <http://www.hmso.gov.uk/acts/acts1998/ 19980029.htm>).

36. *Id.* at §§ 7-15.

37. *Id.* at §§ 16-26.

38. Directive 97/66/EC (1998).

39. Directive 97/66/EC art. 1(2) (1998); *see also* European Commission, *Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 2000C Off. J. of the European Communities 365 E17 (available at <http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/ce365/ce36520001219en02230229.pdf>). [hereinafter "Electronic data protection proposal II"].

40. Directive 97/66/EC, art. 2(d) at 4 (1998). "[S]ervices whose provision consists wholly or partly in the transmission and routing of signals on telecommunications networks, with the exception of radio- and television broadcasting." *Id.*

41. *Id.* at art. 2(a), at 4. "[A]ny natural or legal person who or which is a party to a contract with the provider of publicly available telecommunications services for the supply of such services." *Id.*

ensure a level of security appropriate to the risk presented."[42] In addition, the Telecommunications Privacy Directive required telecommunications service providers to inform their customers of particular security risks:

> In the case of a particular risk of a breach of the security of a network, the provider of a publicly available telecommunications service must inform the subscribers concerning such risks and any possible remedies, including the costs involved.[43]

Thus, the Telecommunications Privacy Directive not only required that telecommunications services take appropriate measures to protect the security of their systems, but also inform their customers of particular risks and available remedies. The Telecommunications Privacy Directive retains the remedies permitted by the Data Protection Directive.[44]

The British implementation of the Telecommunications Privacy Directive was the Telecommunications (Data Protection and Privacy) Regulations 1999 (TDPP Regulations).[45] Like the EU Telecommunications Privacy Directive, the TDPP Regulations applied to a broad class of telecommunications providers and their subscribers.[46] The TDPP Regulations required telecommunications service providers to take "technical and organisational measures which are appropriate to secure the security of the service [they] provide[ ]."[47] When a significant risk to the security of the relevant telecommunications network[48] remained, despite the measures described above, telecommunications service provider were required to inform the affected subscribers of the risk, any appropriate safeguards which the subscribers might take against that risk and the costs involved in the taking of such measures.[49] Finally, the TDPP Regu-

---

42. Directive 97/66/EC art. 4(1) (1998) at 4.

43. Directive 97/66/EC art. 4(2) (1998) at 4.

44. Directive 97/66/EC art. 14(2) (1998) at 7.

45. Telecommunications (Data Protection and Privacy) Regulations (1999) SI 1999/2093.

46. *Id.* at § 2(1). The relevant terms are "telecommunications services provider," meaning a person who provides "services the provision of which consists, in whole or in part, of the transmission and routing of signals on telecommunications networks, not being services by way of radio or television broadcasting;" and "subscriber" meaning a person who is "a party to a contract with a telecommunications service provider for the supply of publicly available telecommunications services." *Id.*

47. *Id.* at § 28(1).

48. *Id.* at § 2(1). "'[R]elevant telecommunications network', in relation to a telecommunications service provider, means a public telecommunications network which is used by that service provider for the provision of publicly available telecommunications services." *Id.*

49. *Id.* at § 28(3).

> Where, *notwithstanding the taking of measures required [above, in subsection 28(1)]*, there is a significant risk to the security of the relevant telecommunications

lations provided persons injured by violations of the regulations with compensation from the violators, subject to the defense that a violator had taken reasonable care to comply with the requirement concerned.[50]

3. *The Electronic Communications Privacy Directive and the British Implementation*

In the meantime, the European Commission proposed the Electronic Communications Privacy Directive to replace and extend the Telecommunications Privacy Directive and adapt the original Data Protection Directive to electronic communications.[51]

Indeed, although the security-related obligations are very similar, the Electronic Communications Privacy Directive has an arguably broader application than the Telecommunication Privacy Directive.[52] The Electronic Communications Privacy Directive covers electronic communications services and their subscribers. The definition of "electronic communication services" covers any service which transmits signals over wire, radio, television, satellite, cable, or by optical or by other electromagnetic means, explicitly including the Internet, except not those providing content or editorial control over the content.[53] Given the already

---

network, the telecommunications service provider shall inform the subscribers concerned of a) that risk; b) any measures appropriate to afford safeguards against that risk which they themselves might take, and (c) the costs involved in the taking of such measures.

Id. [emphasis added].

50. *Id.* at § 35.

51. Directive 2002/58/EC recs. 4-8 at 37-38 (concerning the processing of personal data and the protection of privacy in the electronic communications sector) (available at <http://europa.eu.int/eur-lex/en/com/pdf/2000/en_500PC0385.pdf>). [hereinafter *Electronic data protection proposal I*].

52. *Cf.* Directive 97/66/EC art. 4 (1998) at 4 *with* Directive 2002/58/EC art. 4 (2002) at 43; *see also Electronic data protection proposal I* at 8 (comparing article 4 of the proposed electronic data protection directive with the telecommunications data protection directive; "Unchanged except for replacement of 'telecommunication services' by 'electronic communication services'").

53. Directive 2002/21/EC (March 7, 2002) (describing a common regulatory framework for electronic communications networks and services (Framework Directive), art. 2(a), (c), 2002 O.J. (L 108) 33, 38-39 (available at <http://europa.eu.int/eurlex/pri/en/oj/dat/2002/l_108/l_10820020424 en00330050.pdf>).

> [E]lectronic communications network" means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;
>
> . . .
>
> electronic communications service" means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic

broad scope of the Telecommunication Privacy Directive, it is not clear how much further the new privacy directive extended. For instance, in the view of the UK Information Commissioner's office, the electronic communications revisions may not have been necessary to extend the prior Telecommunications Directive to e-mail.[54]

Using the same language as the Telecommunications Privacy Directive, the Electronic Communications Privacy Directive requires publicly available electronic communications services to take technical and organisational measures to safeguard the security of its services "appropriate to the level of the risk presented."[55] However, the electronic communications privacy directive has a slightly different disclosure requirement:

> In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, *where the risk lies outside the scope of the measures to be taken by the service provider*, of any possible remedies, including an indication of the likely costs involved.[56]

Hence, the Electronic Communications Privacy Directive limits the obligation to provide subscribers information about remedying security risks to those risks that cannot be eliminated by the electronic communications service itself. The Electronic Communications Privacy Directive also retains the remedies permitted by the data protection directive.[57]

The British implementation of the Electronic Communications Privacy Directive (the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PEC Regulations)) superceded the TDPP Regulations in 2003.[58] The PEC Regulations hew very closely to the TDPP Regulations – although, of course, they apply to public "electronic communication services" rather than telecommunication services.[59] The

---

> communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks;

Id.; Council Directive 2002/58/EC, art. 2, 2002 O.J. (L 201) at 43 (incorporating the definitions from the 2002/21/EC directive).

54. U.K. Information Commissioner, *Legal Advice – Telecoms Guidance*, 2-3 (1998) (available at <http://www.dataprotection.gov.uk/dpr/dpdoc.nsf>).

55. Directive 2002/58/EC art. 4(1) (2002) at 43.

56. Directive 2002/58/EC art. 4(2) (2002) at 43.

57. Directive 2002/58/EC art. 15(2) (2002) at 46.

58. Privacy and Electronic Communications (EC Directive) Regulations (2003) SI 2003/2426 § 3.

59. *Id.* at § 2(1) (citing definition of "electronic communications service in Communications Act, 2003, c. 21, § 32(2)).

PEC Regulations also require the implementation of "technical and organisational measures" to secure the communication services,[60] and service providers remain obligated to inform affected subscribers of any remaining security risks, appropriate safeguards which subscribers could take, and the costs involved in the taking of such measures.[61] The PEC Regulations also retain provision of a private right of action for persons injured by their violation.[62]

C. Comparing the Californian and European Approaches to Disclosing Security Breaches

Both California Civil Code section 1798.82 and the disclosure obligations under the European and British data protection regime are far-reaching but, nonetheless, have important limitations.

European disclosure requirements are broad. They apply to the security of the entire network or infrastructure without respect to the nature of the security threat or to the sort of data stored. They apply to all security risks, not just risks to computer systems.

However, two major exceptions may apply: one is explicit, while the other is comparatively ambiguous. First, both Privacy Directives (and their British implementation) apply only to communication service providers, which and only require disclosure of security risks to their customers. Thus, other data collectors are not subject to these regulations (although they are subject to the Data Protection Directive), and the communication service providers have no obligation to disclose breaches to non-customers. Second, "risk" connotes an unrealized contingency, not a realized security breach. The language of the directives appears to contemplate the disclosure of prospective, unrealized security "risks," rather than the disclosure of realized security breaches.[63]. Thus the obligation to disclose security risks might apply only prospectively and not necessarily retrospectively to completed security breaches. (This connotation is heightened with respect to the PEC Regulations, whose disclosure provi-

60. *Id.* at § 5(1).

61. *Id.* at § 5(3).

62. *Id.* at § 30.

63. Directive 2002/58/EC recital 20 (2002) at 39.

> Service providers should . . . inform subscribers of any special risks of a breach of the security of the network . . . It is particularly important for subscribers and users of such services to be fully informed by their service provider of the existing risks which lie outside the scope of possible remedies by the service provider. . . . Service providers who offer publicly available electronic communication services over the Internet should inform users and subscribers of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies. The requirement to inform subscribers of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore normal security level of the service.

sions are limited to risks that cannot be eliminated by the service provider.) It is nonetheless possible to read an obligation to disclose security breaches retrospectively as well as prospectively into the European and British regulations. "Risk" can be read broadly, to apply to both realized events and unrealized contingencies. Further, the discovery of a completed security breach does not extinguish the possibility of additional harm to the confidentiality of data on the network. Indeed, completed security breaches heighten the risk to personal data confidentiality and may fit comfortably within the PEC Regulations' restriction of disclosure to risks that the service provider fails to eliminate. Some commentators have concluded that the TDPP Regulations required disclosure of security breaches after the fact.[64]

Although European rules only apply to service providers, Californian disclosure obligations are less extensive than European standards. The obligation to disclose security breaches to data subjects is restricted by

- the geographical location of the data subjects' residence and the database operators' business operations; and
- the narrow class of protected data.

Some commentators have noted that, while the disclosure requirements under Californian law exclude encrypted data, it does not define encryption or discuss "what type of encryption is sufficient in the event of a security breach. Certain forms of encryption offer limited protection against a security breach."[65] In addition, disclosure to data subjects can be suppressed as long as law enforcement needs or the operator requires to evaluate and repair the security breach. (However, the obligation to disclose security breaches of data containing personal information to the data's owner is less restricted, with respect to encryption or the geographical location of the database operator or the data subjects.)

In both jurisdictions, one available remedy is compensation for the harm caused by a failure to disclose. Although computer database operators might be held separately liable for negligent security in the first place, damages for failure to disclose security breaches would be limited

64. Justin Watts & Hiroshi Sheraton, *Data Protection & Privacy: Even More New Rules* (Sept. 30, 1999) (available at <http://www.bristows.com/articles/detail.asp?frmarticleid=58&frmpdtid=2>).

> Where there remains a significant security risk, providers will be obliged to inform their subscribers of the risks, measures to safeguard against that risk that subscribers might take themselves, and the costs involved in those measures. *For instance, if a service provider discovers that its email system has been hacked and is at risk, it could now be under a statutory obligation to inform its subscribers. Preserving security through maintaining security breaches secret would appear no longer to be an option.*

Id. (emphasis added).

65. Falvey, *supra* n. 1, at 5.

to the harm flowing from depriving other parties the opportunity to mitigate the harm of a security breach. If database operators whose security is breached might face high damages for negligent security but relatively limited damages for failure to disclose subsequent security breaches and little risk of independent discovery such breaches, they might also decide that suppressing the breach would be an economically rationale choice. . Unscrupulous parties might consciously decline to report security breaches, finding that the risk of limited additional liability for failure to disclose outweighed by the possibility of evading greater liability for negligent security.

II. LEGISLATION AND COMMON LAW IMPLICITLY REQUIRING DISCLOSURE OF COMPUTER SECURITY BREACHES

The obligation to disclose security breaches may actually be broader than the existing legislative mandates in California and the EU. Indeed, some preexisting obligations could be found to be tantamount to an obligation to disclose security breaches, even though the preexisting obligations are conceptually distinct from mandates to disclose security breaches. Thus, California's *Security Breach Information Act* and the EU telecommunications and electronic communications privacy directives may not be as groundbreaking as they are now perceived.

There are at least two paradigms where preexisting obligations can be tantamount to requiring disclosure of security breaches. First, the *Data Protection Act* and numerous sector-specific American laws require businesses to provide customers with privacy policies that state how their information will be handled. Also, even American businesses that are not regulated directly increasingly provide their own privacy policies in response to widespread customer concern about privacy and indirect regulation through EU businesses. By definition, unauthorized access to personal data violates these privacy policies with respect to how customer data was supposed to be handled. Other privacy policies may make explicit or implicit representations that the security measures will prevent security breaches. Businesses that negligently fail to recognize and disclose information security breaches to new and continuing customers and data subjects are at least liable for negligent misrepresentation. The second paradigm is simply that some privacy legislation (and conceivably some self-imposed privacy policies) may explicitly require businesses to provide updated, accurate information about the state of their information security policies. Although the language of this legislation clearly contemplates *intentional* modifications to disclosure practices, there are no exceptions for *unintentional* disclosures.

Businesses make representations about their data practices for a variety of reasons. Businesses frequently disclose their data practices vol-

untarily. In two separate targeted surveys ("Random Sampling" and "Most Popular"), the U.S. Federal Trade Commission found that eighty-eight percent and 100 percent, respectively, of respondent Web sites made some form of explicit representation about how they would handle customer data they collected.[66] Moreover, fifty-five percent of respondents in the Random Sampling Survey and seventy-four percent of the respondents in the Most Popular survey specifically made some representation about their security practices with collected data.[67] Voluntary statements about how information will be handled can serve as the basis for negligent misrepresentation, but regulation may play an even more important role in businesses' disclosure of their information practices.

A. American Law

1. *Applicable U.S. Legislation*

Unlike the EU model, there is no universal, comprehensive source of American privacy law. Rather federal American privacy legislation is scattered across a variety of narrowly drafted statutes[68] and at least sixteen states restrict disclosure of data held, variously, by insurance companies, health care providers, financial institutions or other businesses.[69] The statutes discussed here are the *Health Insurance Portabil-*

66. Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress* 10 (May 2000) (available at <http://www.ftc.gov/reports/ privacy2000/privacy2000.pdf>).

67. *Id.* at 19.

68. *See e.g.* Freedom of Information Act, 5 U.S.C. § 552(b)(6), (7) (2003) (restricting public disclosure of information regarding individuals by federal government); Privacy Act of 1974, 5 U.S.C. § 552a (2003) (restricting public disclosure of information regarding individuals by federal government); Fair Credit Reporting Act, 15 U.S.C. § 1681-1681v (2003) (restricting disclosure and use of consumer credit reports); Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-06 (2003) (limiting collection and disclosure of information about children under 13 by website operators); Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809, 6821-6827 (2003) (restricting disclosure of information regarding customers by financial institutions); Electronic Communications Privacy Act of 1986, 18 USCS § 2510-2522, 2701-2712 (2003) (restricting interception and disclosure of electronic communications); Video Privacy Protection Act of 1980, 18 U.S.C. § 2710 (2003) (limiting the disclosure of information about video renters by video rental stores); Drivers' Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-25 (2003) (limiting disclosure of information about drivers by state driver's licensing agencies); Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (2003) (limiting disclosure of information about students by educational institutions); Right to Financial Privacy Act of 1978, 29 U.S.C. §§ 3401-22 (2003) (limiting disclosure of information about customers by depository institutions to federal law enforcement officials); Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §§ 1320d to 1320d-8 (2003); Cable Communication Policy Act of 1984, 47 U.S.C. § 551 (2003) (limiting the disclosure of information about subscribers by cable companies).

69. *See e.g.* Ariz. Rev. Stat. §§ 12-2292 to -2294 (stating confidentiality of patients' medical records and conditions for disclosure); Cal. Civ. Code §§ 56-56.16 (West 2003) (out-

ity and Accountability Act of 1996 ("HIPAA"),[70] the *Children's Online Privacy Protection Act* ("COPPA"),[71] and the *Gramm-Leach-Bliley Act* (GLB).[72]

HIPAA required the Secretary of Health to promulgate standards for maintaining and handling health information in electronic form.[73] HIPAA and the associated regulations protect health information, meaning any information "created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse" which relates to an individual's physical or mental condition, their health care or the future payment for

---

lining patients' rights to their medical records, including restrictions on unauthorized disclosure); Cal. Civ. Code §§ 1798.80-84 (West 2003) (requiring disclosure of unauthorized security breach, and destruction of unneeded business records); Cal. Civ. Code. § 1799.1 (West 2003) (restricting disclosure of bookkeeping records on individual or business); Cal. Health & Safety Code § 123148 (restricting disclosure of patients' clinical laboratory testing results); Conn. Gen. Stat. §§ 36a-41 to -45 (2003) (restricting the disclosure of customers' financial records from financial institutions); Conn. Gen. Stat. §§ 38a-975 to -999a (2003) (describing customers' rights over insurance records, including restrictions on unauthorized disclosure); Fla. Stat. ch. 655.059 (2003) (restricting the disclosure of financial institutions); Idaho Code § 54-1814(13) (2003) (stating physicians subject to discipline for failure to safeguard confidentiality of patient files); 205 Ill. Comp. Stat. § 5/48.1 (2003) (restricting disclosure of customer records by banks, providing customer with notice of such disclosure); Ind. Code §§ 34-43-1-1 to -17 (2003) (noting confidentiality of hospital records); La. Rev. Stat. Ann. § 6:333 (2003) (restricting disclosure of customer records by financial institutions and their affiliates, providing customer with notice of such disclosure); Me. Rev. Stat. Ann. tit. 9-B, §§ 241(13), 242 (2003) (restricting disclosure of customer information by financial institutions, requiring financial institutions to meet privacy requirements of title V of Gramm-Leach-Blilely Act); Me. Rev. Stat. Ann. tit. 22, § 1711-C (2003) (restricting disclosure of patients' health care information); Me. Rev. Stat. Ann. tit. 24-A, §§ 2201-2220 (2003) (customers' rights with respect to information collected by insurers, including restrictions on unauthorized disclosure); Md. Code Ann., Fin. Inst. § 1-301 to -305 (2003) (restricting disclosure of customer information by financial institutions); Mass. Gen. Laws ch. 167B, § 16 (2003) (restricting disclosure of account information or information relating to electronic fund transfers, and requiring procedures to ensure information security and inform customer of unauthorized disclosure of information); Mass. Gen. Laws ch. 175I, § 1-22 (2003) (customers' rights over insurance records, including restrictions on unauthorized disclosure); Mont. Code Ann. §§ 33-19-101 to -106, 33-19-201 to -206, 33-19-301 to -308, 33-19-401 to -409 (customers' rights over insurance records, including restrictions on unauthorized disclosure); Or. Rev. Stat. §§ 746.665, 746.680, (2003) (restricting disclosure of information collected from customers by insurance companies); R.I. Gen. Laws §§ 5-37.3-1 to -11 (2003) (restricting disclosure of patients' confidentiality health care information); Wis. Stat. §§ 146.80-146.84 (2003) (customers' rights over medical records, including restrictions on unauthorized disclosure).

70. Pub. L. No. 104-191, § 262, 110 Stat. 1936, 2021-31 (1996).

71. Pub. L. No. 105-277, §§ 501-510, 112 Stat. 2681-728 to -735 (1998).

72. Pub. L. No. 106-102, §§ 1301-08, 113 Stat. 1338, 1436-45 (1998).

73. 42 U.S.C. §§ 1320d-1, 1320d-2 (2003); *see also* 42 U.S.C. §§ 1320d, 1320d-3 to 1320d-8 (2003).

health care.[74] HIPAA applies to health plans,[75] health care clearinghouses[76] and those health care providers[77] that transmit health information electronically.[78] HIPAA regulations generally restrict the disclosure of health information,[79] but provide exceptions where treatment requires disclosure,[80] where authorization is obtained,[81] where the data subject has an opportunity to object[82] and where no authorization or opportunity to object is required.[83] Most data subjects have a right to notice of the disclosures that may be made by "the covered health plan, health care provider or clearinghouse."[84] A covered entity is required to "promptly revise and distribute its notice whenever there is a material change to the uses or disclosures . . . or other privacy practices stated in the notice" before the planned change is implemented.[85] Moreover, data subjects have a right to request an accounting of all disclosures of health information by a covered entity.[86] The covered entity must include, for each disclosure, the date of the disclosure, the name and address of the person receiving the information, a description of the information disclosed and the purpose of the disclosure.[87] The Secretary of Health and Human Services enforces HIPAA by imposing fines on negligent violationsand providing for criminal penalties for knowing disclosure.[88]

COPPA restricts and protects individually identifiable information[89] collected from children under thirteen years old[90] by operators of Web

74. 42 U.S.C. § 1320d(4); 45 C.F.R. § 160.103 (2003).
75. 42 U.S.C. § 1320d(5); 45 C.F.R. § 160.103 (2003).
76. 42 U.S.C. § 1320d(2); 45 C.F.R. § 160.103 (2003).
77. 42 U.S.C. § 1320d(3); 45 C.F.R. § 160.103 (2003).
78. 42 U.S.C. § 1320d-1(a); 45 C.F.R. § 160.102(a) (2003).
79. 45 C.F.R. §§ 160.502, 164.504 (2003).
80. 45 C.F.R. § 160.506 (2003).
81. 45 C.F.R. § 160.508 (2003).
82. 45 C.F.R. § 160.510 (2003).
83. 45 C.F.R. § 160.512 (2003).
84. 45 C.F.R. § 160.520(a), (b)(1) (2003).
85. 45 C.F.R. § 160.520(b)(3) (2003).
86. 45 C.F.R. § 160.528(a) (2003).
87. 45 C.F.R. § 160.528(b)(1), (2) (2003).
88. 42 U.S.C. § 1320d-5 (2003) (providing for fines up to $100 per violation, capped at $25,000 per year and to be waived or reduced for reasonable cause for violations); 42 U.S.C. § 1320d-5 (2003) (providing for fines up to $250,000 and imprisonment for up to 10 years for knowing violations by access or disclosure of individually identifiable health information).
89. 15 U.S.C. § 6501(8) (2003) (including name, address, e-mail address, telephone number, Social Security number and other information collected with it); 16 C.F.R. § 312.2 (2003) (including persistent identifiers, such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information and a combination of a last name or photograph of the individual with other information such that the combination permits physical or on-line contacting).
90. 15 U.S.C. § 6501(1) (2003); 16 C.F.R. § 312.2 (2003).

sites which are directed at children, or who have actual knowledge they are collecting information from children.[91] As part of the restrictions on collection and disclosure, Web site operators must provide notice of what information is collected from children, how it is used and how it is disclosed.[92] The Federal Trade Commission has provided specific regulations on the content and form of notice, including the planned use of the information and whether personal information is disclosed to third parties.[93] Particular provision is made for parental notice and consent, "including notice of any material change in the collection, use, and/or disclosure practices to which the parent has previously consented."[94] Compliance with COPPA or its subsidiary regulations is enforced by the Federal Trade Commission.[95]

GLB's subsidiary privacy regulations are promulgated and enforced by a variety of federal agencies, including the Federal Trade Commission.[96] GLB regulations protect nonpublic personal information[97] from disclosure by financial institutions.[98] GLB largely prohibits disclosure of personal information to unaffiliated third parties[99] without providing

91. 15 U.S.C. §§ 6501(2), 6502(a)(1) (2003); 16 C.F.R. § 312.2 (2003).

92. 15 U.S.C. § 6502(b)(1)(A)(i) (2003).

93. 16 C.F.R. § 312.4(b)(2) (2003).

94. 16 C.F.R. § 312.4(c) (2003).

95. 16 C.F.R. § 312.9 (2003); *see also* 15 U.S.C. § 57a, 57b (2003) (defining procedure for unfair or deceptive trade practice enforcement, providing remedies of rescission or reformation of contracts, the refund of money or return of property, the payment of damages, and public notification, but not exemplary or punitive damages).

96. 15 U.S.C. §§ 6804-05 (2003) Generally, the Office of the Comptroller of the Currency regulated banks with a national charter, the Board of Federal Reserve regulates banks in the federal reserve system, the Board of the Federal Deposit Insurance Corporation regulates banks with FDIC insurance (not otherwise regulated by the OCC), the Security Exchange Commission regulates a variety of securities-related businesses, state insurance commissioners regulate insurance and the FTC regulates any other "financial institution," as defined under 12 U.S.C. § 1843(k) (2003). *Id.*; *see also e.g.* 12 C.F.R. § 40.1-40.18 (2003) (following GLB privacy regulations of OCC); 12 C.F.R. §§ 216.1-.18 (2003) (following GLB privacy regulations of Federal Reserve); 12 C.F.R. §§ 332.1-.18 (2003) (following GLB privacy regulations of FDIC).

97. *See e.g.* 15 U.S.C. § 6802(a) (2003) (restricting disclosure of personally identifiable financial information); 15 U.S.C. § 6809(4) (2003); 16 C.F.R. § 313.3(n) (2003) (meaning personally identifiable financial information that is not public); 16 C.F.R. § 313.3(o) (2003) (stating that publicly available to the general public means now or about to be available through federal, state or local government, or in widely distributed media); 16 C.F.R. § 313.3(p) (2003) (noting that personally identifiable financial information is information obtained about a consumer in the course of providing financial services or products to that consumer).

98. *See e.g.* 15 U.S.C. § 6802(a) (2003) (restricting information disclosure by financial institutions); 15 U.S.C. § 6809(3) (2003); 16 C.F.R. § 313.3(k) (2003) (meaning any of a broad range of entities defined under 12 U.S.C. § 1843(k)).

99. 15 U.S.C. § 6809(3) (2003); *see also* 16 C.F.R. § 313.3(a), (g) (2003) (noting unaffiliated meaning not having control by ownership, control, or power to vote twenty-five per-

prior notice to the data subject[100] and providing opportunity to opt out of the disclosure.[101] GLB privacy notices must be given to consumers before disclosing personal information to others, to new customers or when providing customers with a new service or product and at least annually to existing customers.[102] Privacy notices are required to include

- the categories of nonpublic personal information which are collected and disclosed;
- the categories of affiliates and nonaffiliated third parties that receive nonpublic personal information from the financial institution; and
- the financial institution's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.[103]

At the state level, Connecticut, Maine and Massachusetts also require disclosure of treatment of personal information by insurers in addition to the obligations under GLB.[104]

HIPAA, COPPA and GLB have gained notoriety because they impose security requirements on the regulated businesses. COPPA and its subsidiary regulation simply require Web site operators to "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."[105] GLB generally provides that the various GLB regulators should promulgate

> appropriate standards. . . relating to administrative, technical and physical safeguards to insure the security and confidentiality of customer records and information; to protect against any anticipated threats or hazards to the security or integrity of such records; and to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[106]

The Secretary of Health and Human Services has generated an extensive, detailed set of specific security requirement for health plans, health information clearinghouses and certain health care providers

---

cent or more of the voting shares of a company, directly or indirectly, control over the election of a majority of the directors or management; or the power to exercise, directly or indirectly, a controlling influence over the management or policies of the company).

100. 15 U.S.C. § 6802(a), (e) (2003) (stating prohibition and variety of exceptions to prohibition on disclosure); 16 C.F.R. §§ 313.8(a), 313.10(a), 313.13-.15 (2003) (stating general prohibitions and exceptions).

101. 15 U.S.C. § 6802(b) (2003); 16 C.F.R. § 313.7 (2003).

102. 16 C.F.R. §§ 313.4(a), (d), 313.5 (2003).

103. 16 C.F.R. § 313.6(a)(1), (2), (3), (8) (2003).

104. Conn. Gen. Stat. §§ 38a-979, 38a-988 (2003); Me. Rev. Stat. Ann. tit. 24-A, §§ 2206, 2215 (2003); Mass. Gen. Laws ch. 175I, §§ 4, 13 (2003).

105. 15 U.S.C. § 6502(b)(1)(D) (2003).

106. 15 U.S.C. § 6801(b) (2003).

under HIPPA.[107] Although none of these regulations explicitly address disclosing security breaches to data subjects, the official Interagency Guidance to the GLB regulations explicitly discusses disclosure of security breaches to customers.[108] The Interagency Guidance "describes the [regulating] Agencies' expectations that every financial institution develop a response program to protect against and address reasonably foreseeable risks associated with internal and external threats to the security of customer information maintained by the financial institution or its service provider."[109] With respect to disclosure of security breaches to customers, the Interagency Guidance stated:

> Under the Security Guidelines, financial institutions have an affirmative duty to protect their customers' information against unauthorized access or use. An institution may not forgo notifying its customers of an incident because the institution believes that it may be potentially embarrassed or inconvenienced by doing so. . . . If the institution is able to determine from its logs or other data precisely which customers' information was accessed or misused, it may restrict its notification to those individuals. However, if the institution cannot identify precisely which customers are affected, it should notify each customer in groups likely to have been affected, such as each customer whose information is stored in the group of files in question. . . . An institution should notify affected customers whenever it becomes aware of unauthorized access to sensitive customer information unless the institution, after an appropriate investigation, reasonably concludes that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of affected customers, including by monitoring affected customers' accounts for unusual or suspicious activity.[110]

Moreover, as described below HIPAA and COPPA likely also imply a duty to disclose security breaches to affected data subjects.

HIPAA, COPPA and GLB require businesses to provide data subjects with accurate information about who will have access to personal information related to them as the businesses collect the information. Moreover, regulated businesses must provide continuous, updated information on the disclosure of personal data. COPPA and HIPAA require businesses to inform data subjects (or their parents) of "material changes" to their disclosure policies. HIPAA further requires businesses

107. 42 U.S.C. § 1320d-2(d) (2003) (requiring regulations on security); Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334 (to be codified at 16 C.F.R. §§ 164.302-.318). For instance, HIPAA's security rule requires implementation of thorough assessments of the potential security vulnerabilities of protected health information and procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. 16 C.F.R. §§ 164.308(a)(1)(ii)(A) (2003).

108. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 68 Fed. Reg. 47,954 (Aug. 12, 2003).

109. *Id.* at 47,955.

110. *Id.* at 47,959-960.

to provide data subjects an accounting of who had access to their personal health information on request. GLB requires updated representations about how information will be handled at least annually, and every time a customer uses a new financial service or product. Those HIPAA, COPPA and GLB provisions which require covered entities to provide data subjects with updated information about the treatment of their data, contemplate intentional, planned changes to privacy policies, but do not exclude hostile, unplanned security breaches. A covered business's failure to prospectively disclose security breaches in which computer criminals had access to protected data would probably violate the provisions above.

2. *Fraudulent and Negligent Misrepresentation*

Data subjects also rely on the representations businesses make about how they handle data, even when those representations are mandated by HIPAA, COPPA and/or GLB. The reliance is protected under common law (it is important to note that HIPAA, COPPA and GLB preempt inconsistent or contrary state law).[111] However, it is unlikely that any common law to make accurate or truthful representations would be held inconsistent with these privacy statutes. In addition, HIPAA[112] and GLB[113] preemptions expressly do not apply to state law requirements that offer more protection than their own provisions).

Fraud is "a misrepresentation of fact, opinion, intention or law for the purpose of inducing another to act or to refrain from action in reliance upon it" and a person is liable for fraud to the extent of the pecuniary loss caused by the other party's "justifiable reliance upon the misrepresentation."[114] Fraud can extend not only to past and present statements of facts, but also to promissory statements (such as the prospective disclosure and use of personal information).[115] Moreover, statements which are truthful but known to be misleading because they omit additional, qualifying matters are fraudulent misrepresentations.[116] The privacy disclosures under HIPAA, COPPA and GLB are intended to help data subjects make informed choices about how they share their infor-

111. 42 U.S.C. § 1320d-7(1) (2003); 15 U.S.C. § 6502(d) (2003); 15 U.S.C. § 6807(a) (2003).

112. 42 U.S.C. § 1320d-7(2) (2003); 45 C.F.R. § 160.203(b). *See also* 45 C.F.R. § 160.202 "With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information." *Id.*

113. 15 U.S.C. § 6807(a) (2003). *See also* 15 U.S.C. § 6807(b) (permitting the FTC to designate particular state law provisions as offering more protection than the GLB provisions).

114. *Restatement (Second) of Torts* § 525 (1965).

115. *Id.* at § 525, cmt. f.

116. *Id.* at §§ 529, 551 (1965).

mation. To that end, privacy disclosures influence data subjects' choices. Thus, businesses that knowingly conceal security breaches from new and continuing customers while they represent to data subjects that disclosure of personal information is restricted are committing fraud on those data subjects.

Liability for negligent misrepresentation attaches where a person

- in the course of his business, or other transaction in which he has a pecuniary interest;
- failing to exercise reasonable care;
- supplies false information for the guidance of the other party in its business transactions; and
- the other party suffers loss from justifiable reliance on that information.[117]

However, the damages recoverable in an action for negligent misrepresentation are limited to the loss suffered

- by the person or class of persons for whose benefit and guidance the representor intends to supply the information; and
- through reliance upon it in a transaction that he intends the information to influence, except that
- the liability of one who is under a public duty to give information extends to the loss suffered by any of the class of persons for whose benefit the duty is created, in any of the transactions in which it is intended to protect them.[118]

Private individuals or corporations who are required by law to file information for the benefit of the public are under a "public duty."[119]

Again, businesses disclose their privacy policies to induce data subjects into transactions with the business and into providing them with information. Businesses subject to HIPAA, COPPA or GLB have a duty to give information to data subjects for their protection; those businesses are liable for damages suffered through transactions involving privacy policy disclosures from false statements negligently made. When privacy policies make representations that the disclosure of data subject's personal information is restricted, businesses subject to HIPAA, COPPA or GLB have a duty to ensure that those representations are accurate.

Again, businesses disclose their privacy policies in part to induce data subjects into transactions with the business and into providing them with information. Businesses subject to HIPAA, COPPA and GLB have a duty to explain their data practices to data subjects; those businesses are liable for damages caused by negligently inaccurate privacy policy disclosures. Although the following cases do not relate to *disclo-*

117. *Id.* at § 552(1) (1979).
118. *Id.* at § 552(2), (3).
119. *Id.* at § 552 cmt. k.

sure of information security breaches (but rather to the breaches themselves), the Federal Trade Commission's actions against Eli Lilly, Microsoft, Guess, and Tower Records over the disparities between their announced privacy policies and their actual information practices show that already-existing standards of deception can be applied to representations regarding information security practices. The Federal Trade Commission has the ability to prevent "unfair or deceptive acts or practices in or affecting commerce" under section 5(a) of the *Federal Trade Commission Act*.[120] In all these settlements, the Federal Trade Commission alleged that the disparities between the stated and actual information practices were unfair and deceptive. In particular, Eli Lilly's privacy policy stated it would protect the confidentiality of its customer's personal information, but mistakenly disclosed the e-mail addresses of 669 subscribers of information services provided in connection with Eli Lilly's Prozac.com Web site.[121] In Microsoft's case, its privacy policy stated that its various .NET Passport services were protected by "powerful online security technology" and did not collect personal information, while actually these services failed to provide adequate security measures.[122] While Guess's privacy policy stated it would take reasonable technical measures to secure customer information (including encrypting personal information), its Web site was vulnerable to "SQL injection attacks" that were "commonly known in the information technology industry" since 1997 and Guess did not, in fact, encrypt personal data.[123] These companies most likely implemented their privacy policies voluntarily, not under a particular privacy statute – but nonetheless faced liability because their information security practices did not meet their representations to their customers.

New York's Attorney General has also pressed companies on privacy policies. When Internet publisher Ziff Davis gathered customer information under a privacy policy that promised "reasonable security," but left approximately 12,000 subscription orders exposed on the Internet, which in turn led to incidents of identity theft, the New York Attorney General

120. 15 U.S.C. § 45(a) (2003).

121. Federal Trade Commission, *In the Matter of Eli Lilly and Company*, <http://www.ftc.gov/os/ 2002/05/elililly cmp.htm> (Jan. 18, 2002); *see also* Federal Trade Commission, *Eli Lilly Settles FTC Charges Concerning Security Breach*, <http://www.ftc.gov/opa/2002/01/elililly.htm> (Jan. 18, 2002).

122. Federal Trade Commission, *In the Matter of Microsoft, Inc.*, <http://www.ftc.gov/os/2002/12/ microsoftcomplaint.pdf> (Aug. 8, 2002); *see also* Federal Trade Commission, *Microsoft Settles FTC Charges Alleging False Security and Privacy Promises*, <http://www.ftc.gov/opa/2002/08/ microsoft.htm> (Aug. 8, 2002).

123. Federal Trade Commission, *In the Matter of Guess?, Inc.*, <http://www.ftc.gov/os/2003/06/ guesscmp.pdf> (June 18, 2002); *see also* Federal Trade Commission, *Guess Settles FTC Security Charges; Third FTC Case Targets False Claims about Information Security*, <http://www.ftc.gov/opa/2003/06/guess.htm> (June 18, 2002).

fined Ziff Davis approximately $25,000 and required a number of new security measures.[124] Victoria's Secret's customers billing details could be downloaded from Victoria's Secret's Web site, despite provisions in the Web site privacy policy that "[a]ny information you provide to us at this site when you establish or update an account, enter a contest, shop online or request information . . . is maintained in private files on our secure web server and internal systems . . . ."[125] Victoria's Secret settled the subsequent deceptive advertising lawsuit by the New York Attorney General by agreeing to implement certain reforms and paying New York a $50,000 settlement.[126] Likewise, the American Civil Liberties Union settled over an incident where consumer's personal information was available in a security breach in its Web site (even though it was operated by a third party vendor) contrary to specific representations in the ACLU's privacy policy.[127] Finally, the bookseller Barnes and Noble entered into a settlement with the New York Attorney General because of security vulnerabilities in its website that "permitted unauthorized access to consumers' accounts and personal information and enabled users to make purchases on the site from consumers' accounts."[128] Regardless of why these companies chose to make representations about their information security practices, they were held responsible for the inaccuracy of those representations based on pre-existing laws.

B. British Law

1. *Data Protection Act of 1998*

The *Data Protection Act 1998* (the "DPA") is another example of legislation that requires businesses to make representations about their information practices. Businesses that fail to mention information security breaches while making representations under the DPA can be held liable, either under the DPA itself or for fraud or negligent misrepresentation. As with American privacy law, the end result is that liability for suppressing security breaches flowing from the disclosures required by the DPA (which affect nearly any commercial entity that gathers data)

124. Office of the New York State Attorney General, *Major Tech Publisher Reaches Agreement With Attorney General On E-Commerce Security Safeguards*, <http://www.oag.state.ny.us/press/2002/aug/aug28a_02.html> (Aug. 28, 2002).

125. Office of the New York State Attorney General, *Victoria's Secret Settles Privacy Case*, <http://www.oag.state.ny.us/press/2003/oct/oct21b_03.html> (Oct. 21, 2003).

126. *Id.*

127. Office of the New York State Attorney General, *State Settles Online Privacy Case*, <http://www.oag.state.ny.us/press/2003/jan/jan14a_03.html> (Jan. 14, 2003).

128. Office of the New York State Attorney General, *Attorney General Reaches Agreement With Barnes And Noble On Privacy And Security Standard*, <http://www.oag.state.ny.us/press/2004/apr/apr29a_04.html> (Apr. 29, 2004).

has a much broader scope than any disclosure required under the PEC Regulations (which applies only to communication service providers).

The DPA requires data controllers to adhere to the EU data protection principles[129] with respect to personal data.[130] The first data protection principle requires personal data be processed "fairly and lawfully."[131] Under the first principle, when businesses obtain personal data, they typically must inform the data subject of "the purposes for which the data are intended to be processed."[132] The second principle provides that data can be used "only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes."[133] Thus, when British businesses obtain personal data, they make a binding representation of the intended uses of that data.

Thus, businesses are typically required to inform data subjects they are collecting personal data and to specify the particular purpose for which the data will be used. Security breaches are inherently "incompatible" with the intended purposes specified in the notice to data subjects.[134] Although data subjects damaged by intruders' access to their data might have a cause of action under the DPA because the intruders' access was "incompatible" with the purpose for which the business originally collected the data, this does not mandate a *disclosure* of the same security breach.

The DPA might implicitly require disclosure of security breaches in three ways. The DPA restricts the collection of data under misleading circumstances, requires data controllers to describe their security measures to the Information Commissioner and requires data controllers to tell data subjects to whom their data has been disclosed on request.

---

129. Data Protection Act 1998, ch. 29, § 4(4) (noting that data controllers must comply with data protection principles); *id.* at sched. 1, pt. I, ¶ 1 (stating that personal data must be processed "lawfully and fairly"). [hereinafter "DPA"].

130. *Id.* at § 1. Personal data is data "which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller." *Id.*

131. *Id.* at sched. 1, pt. I, ¶ 1 (data must be processed "lawfully and fairly").

132. *Id.* at sched. 1, pt. II, ¶ 2; *but see id.* sched. 1, pt. II, ¶ 3 (stating exceptions for disproportionate effect and other legal obligations).

133. *Id.* at sched. 1, pt. I, ¶ 2; *see also id.* sched. 1, pt. II, ¶ 5 (noting that the purpose for data collection may be specified by a notice to the data subject when the data is obtained or by notification to the Information Commissioner).

134. *Id.* at sched. 1, pt. II, ¶ 6.

> In determining whether any disclosure of personal data is compatible with the purpose or purposes for which the data were obtained, regard is to be had to the purpose or purposes for which the personal data are intended to be processed by any person to whom they are disclosed.

Id.

First, one of the criteria for compliance with the first principle is whether the data were obtained by deception or misrepresentation regarding the purposes for which the data were required.[135] While the DPA's language contemplates intentional deception regarding the data, not unintended security breaches, the DPA might also require disclosure of known, ongoing security breaches. (This may depend on whether the word "purpose" is read to refer only to the data collector's use of the data, or extends to others' intended use or uses unintended by the data collector.) This would not necessarily require the disclosure of *past* information security breaches.

Second, the DPA requires data controllers to prepare "notifications" as part of registering[136] with the Information Commissioner, subject to criminal penalties.[137] As part of notification, data controllers must provide "a general description" of the technical and measures taken against unauthorized use or destruction of personal data.[138] Moreover, data controllers must update their descriptions of security measures as soon as practicable, but no later than twenty-eight days from the date the description becomes incomplete or inaccurate.[139] It may be possible to describe the measures taken to respond to a security breach without disclosing the security breach itself, but such descriptions would doubtless damage the credibility of the data controller's good faith compliance with the DPA.

Finally, data subjects have a right to information from data collectors that includes a description of "recipients or classes of recipients to whom [their data] are or may be disclosed" on written request.[140] Again, the DPA obviously contemplates intentional disclosures, but nothing in the DPA's language exempts data controllers from disclosing that unknown (or known) computer criminals absconded with a data subject personal data. Data subjects have a right to compensation for damage caused by a violation of the DPA.[141] However, the DPA is not a strict liability regime: data controllers are not liable where they can prove that

135. *Id.* at sched. 1, pt. II, ¶ 1. "In determining for the purposes of the first principle whether personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed." *Id.*

136. *Id.* at §§ 17-19, 21; *but see* Data Protection (Notification and Notification Fees) Regulations 2000 SI 2000/188 at § 3, sched. 1, ¶¶ 2-5 (available at <http://www.legislation.hmso.gov.uk/si/si2000/20000188.htm>) (noting that certain exceptions for staff administration, advertising and marketing to prior customers, accounts and records, and non-profit organizations).

137. DPA at § 60.

138. *Id.* at § 18(b)(2); *Id.* at sched. 1, pt. I, ¶ 7.

139. *Id.* at § 20(1), (2).

140. DPA at § 7(1), (2).

141. *Id.* at § 13(1).

they "had taken such care as in all the circumstances was reasonably required to comply with the requirement concerned."[142]

2. *Deceit and Negligent Misrepresentation*

Regardless of the direct implications of the DPA, data controllers' representations about who will have access to the data subject's personal information are subject to common law liability for deceit and negligent misrepresentation. The elements of deceit are

- that a material, untrue representation was made;
- with the knowledge or belief that it was untrue, or was made recklessly, careless whether it was true or false;
- the representation was made, with the intention that the other part should rely on it;
- that the other party did, in fact, rely upon the representation; and
- that the other party suffered a loss as a result.[143]

Businesses obtaining personal data under the DPA must make binding representations about the data's intended use. The data protection principles typically require businesses to collect data either with the data subjects' consent or under the stipulation that collecting the data is a necessary part of an actual or intended contract to which the data subject is party.[144] Thus, representations describing the intended use of data to data subjects under the DPA are a practical precondition to obtaining the consent necessary to collect personal data. As the above disclosures induce data subjects to acquiesce to an underlying transaction, they are material representations[145] and they are made with the intention of having the data subjects rely on them.[146] While these representations concern prospective uses of personal information, this is not an absolute barrier to liability for deceit; the representation may imply that there are facts to support the representation.[147] At the least, businesses

142. *Id.* at § 13(3).

143. *Jaffray & Ors v. Society of Lloyd's*, EWCA Civ. 1101, ¶ 49 (July 26, 2002) (available at <http://www.bailii.org/ew/cases/EWCA/Civ/2002/1101.html>).

144. *See* DPA at sched. 1, pt. I, ¶ 1 (requiring at least one schedule 2 condition to be met); *Id.* at sched. 2, ¶¶ 1-6 (noting that data can be collected where the user consents, the data is needed for a contract or an intended contract at the data subject's request, where necessary to protect the vital interests of the data subject, where necessary for the administration of justice or execution of a specific law, and the legitimate interests of the data controller, as defined by the Secretary of State).

145. *Jaffray,* EWCA Civ. 1101 at ¶ 60. "A representation is material when its tendency, or its natural and probable result, is to induce the representee to act on the faith of it in the kind of way in which he is proved to have in fact acted." *Id.*

146. *Id.* at ¶¶ 66-67.

147. *Id.* at ¶¶ 50-59 (citing *Barings Plc v. Coopers & Lybrand*, EWHC 461, ¶¶ 46-50 (2002) (available at <http://www.bailii.org/ew/cases/EWHC/Ch/2002/461.html>).

can be held liable if they recklessly or carelessly fail to disclose the possibility of security breaches to data subjects on a prospective basis.

Moreover, businesses that have a duty of care in making a statement of fact, or opinion and fail to exercise that care can be liable for negligent misrepresentation under *Hedley Byrne & Co., Ltd. v. Heller & Partners Ltd.*[148] Establishing negligent misrepresentation requires proof of

- a duty of care to make accurate statements;
- a breach of that duty (i.e., that the misrepresentation was both false and would not have been made by a person exercising reasonable care);
- the plaintiff's reliance on the same representations; and
- the loss suffered fell within the scope of the defendant's duty.[149]

Hedley stated that the duty of accuracy in representation can arise from contract or fiduciary duties, or where the defendant has another special relationship to plaintiff.[150] The most common issue in establishing liability for negligent misrepresentation is whether a duty of care for misstatements should extend to the defendant where no contract or fiduciary duty exists.[151] The most recent development of this point of law is *Caparo Industries plc v. Dickman*.[152] *Caparo* posits three elements for finding a special relationship: foreseeability that the plaintiff (or a class including the plaintiff) would rely and be harmed by the statement, proximity between the plaintiff and defendant, and whether it was fair, just, and reasonable to impose liability.[153] Businesses' privacy policies are susceptible to liability for negligent misrepresentation and fraud because the policies induce customers and data subjects to supply data or consent to data collection and customers and data subjects rely on the businesses' privacy policies.

Customers who entered into contracts under the auspices of a privacy policy that fraudulently or negligently misrepresents how the data were handled can rely on the *Misrepresentations Act 1967*.[154] Under the *Misrepresentations Act*, the business is liable when a customer suffers a loss because of negligent misrepresentation regarding the privacy poli-

148. [1964] A.C. 465 (H.L. 1963).

149. *See e.g. Hagen v. ICI Chemicals & Polymers Ltd.*, IRLR 31 (Q.B. 2001).

150. *Hedley*, [1964] A.C. at 502, 528-529; *see id.* (Hodson, L.J.) (discussing a "special relationship" as the basis for a duty of accurate representation).

151. *See* Christian Witting, *Justifying Liability to Third Parties for Negligent Misstatements*, 20 Oxford J. Legal Stud. 615 (2000) (discussing "perpetually frustrating" problem of when to extend duty of accuracy in representation to a party).

152. [1990] 2 A.C. 605 (H.L. 1990).

153. *See id.* at 621, 629, 638, 658, 662; *see also* Witting, *supra* n. 141 (describing the rationale of extending the duty of accuracy because the representor induced the plaintiff to rely on the representation).

154. Misrepresentations Act 1967, ch. 7.

cies, unless the business proves it had "reasonable ground to believe[,] and did believe[, that] up to the time the contract was made the facts represented were true."[155] Thus, the *Misrepresentation Act* shifts the burden of proof onto the business.

If any business subject to the DPA negligently fails to recognize or simply willfully refrains from disclosing a security breach, but continues to collect data from data subjects under a misleading representation, the business can be held liable for negligent misrepresentation or fraud.

C. Other Commonwealth Law

Two other Commonwealth jurisdictions, Canada and Australia, have legislation that directly and indirectly implicates a duty to disclose information security breaches. Both Canada and Australia have comprehensive privacy legislation, similar to the United Kingdom's DPA (Other financially significant jurisdictions with privacy legislation similar to the DPA include Eire (Ireland),[156] the Isle of Man,[157] and Jersey.)[158] In Canada, the *Personal Information Protection and Electronic Documents Act 2000* (PIPEDA) protects the disclosure and use of customer and employee information in selected industries.[159] In Australia, the *Privacy Act 1988*, as amended by the *Privacy Amendment (Private Sector) Act 2000*, protects personal information of identifiable individuals and covers a wide variety of entities (with some technical exceptions).[160] In both cases, the legislation requires representations to data subjects that can dovetail with existing common law doctrines of fraud and negligent misrepresentation when an information security breach is not disclosed.

---

155. *Id.* at § 2(1).

156. *See* Data Protection Act 1988, ch. 25 (Eire) (available at <http://www.dataprivacy.ie/6ai.htm>); *see also* Office of the Irish Data Protection Commissioner (available at <http://www.dataprivacy.ie>).

157. *See* Data Protection Act 2002, ch. 2 (Isle of Man) (available at <http://www.gov.im/infocentre/acts/pdfs/dpa2002.pdf>); *see also* Isle of Man Government Office of the Data Protection Supervisor (available at <http://www.gov.im/odps/>).

158. *See* Data Protection (Jersey) Law 1987, ch. 12 (available at <http://www.Jerseylegalinfo.je/Law/LawsInForce/htm/LAWFILES/1987/default.asp?URL=Jersey_Law_12-1987.htm>); *see also* Office of the Data Protection Registrar (available at <http://www.dataprotection.gov.je>).

159. Personal Information Protection and Electronic Documents Act, 23 C. Gaz. 1, ch. 5 (2000) (Can.) (available at <http://laws.justice.gc.ca/en/P-8.6/>) [hereinafter "PIPEDA"].

160. Privacy Act, 1988, c. 119 (Austl.), amended by Privacy Amendment (Private Sector) Act 2000, c. 155 (Austl.) (available at <http://www.privacy.gov.au/publications/privacy88_240103.doc>).

1. *Canadian Personal Information Protection and Electronic Documents Act 2000*

PIPEDA governs personal information collected, used or disclosed by associations, partnerships, trade unions or persons in the course of commercial activity.[161] PIPEDA also governs personal employee information collected, used or disclosed by a variety of interprovincial firms including transportation firms, telegraph operators, radio stations, and banks.[162] "Personal information" is broadly defined as "information about an identifiable individual," but excludes an employer's directory information.[163] PIPEDA requires covered entities to comply with the principles set out in the National Standard of Canada, *Model Code for the Protection of Personal Information*,[164] with certain exceptions.[165] PIPEDA requires covered entities to adopt internal grievance policies to resolve complaints by data subject.[166] Afterwards, data subjects can bring allegations of PIPEDA violations before the Privacy Commissioner, who determines the complaints' validity.[167] Plaintiffs must bring their allegations of PIPEDA violations before the Privacy Commissioner before they can sue in Canadian federal court.[168] The court may order entities to correct their practices and can "award damages to the complainant, including damages for any humiliation that the complainant has suffered."[169]

Under PIPEDA, covered entities have a general obligation to make binding representations about how personal information is used or disclosed. Under the *Model Code*, covered entities are required to identify the "purposes for which personal information is collected" and to document those purposes.[170] Entities are limited to the uses or disclosures of personal information which they identified at or prior to collection,[171] and they must also generally obtain the data subject's consent.[172] When an entity seeks to put previously collected personal information to a new

161. PIPEDA, §§ 2(1), 4(1)(a).

162. *Id.* at §§ 2(1), 4(1)(b).

163. *Id.* at § 2(1).

164. *Id.* at § 5(1), sched. 1.

165. *Id.* at § 5(1), 7-9 (including various exceptions for exigent or emergency circumstances, frustration of law enforcement investigations, collection for statistical, journalistic, artistic or literary purposes, scholarly study or research, collection of publicly available information, debt collection, response to a valid subpoena, certain investigatory procedures related to money-laundering, in cases that implicate Canadian national security or otherwise required by law).

166. *Id.* at sched. 1, ¶ 4.10.

167. *Id.* at §§ 11-13.

168. *Id.* at § 14.

169. *Id.* at § 16(a), (c).

170. *Id.* at sched. 1, ¶¶ 4.2, 4.2.1 (citing *id.* at sched. 1, ¶ 4.9).

171. *Id.* at sched. 1, ¶ 4.2.2 (citing *id.* at sched. 1, ¶ 4.4).

172. *Id.* at sched. 1, ¶¶ 4.3-4.3.8.

use, it must identify the new use and obtain consent of the data subject beforehand.[173] The Model Code generally prohibits entities from using or disclosing personal information for purposes inconsistent with those previously identified to data subjects.[174] While PIPEDA and the Model Code do not contemplate inadvertent disclosures, it is clear that information security breaches would be inconsistent with previously identified uses or disclosures for personal information. Moreover, the *Model Code* has explicit (if vague) security requirements, which require entities to adopt physical, technical and organisational security safeguards "appropriate to the sensitivity of the information" maintained.[175] However, it does not appear to be a strict liability statute, at least with respect to the Privacy Commissioner's action in cases alleging breach of PIPEDA's security provisions.[176] These requirements do not require disclosure of security breaches.

While security breaches might violate the provisions of *Model Code* and PIPEDA described above, they do not explicitly mandate the disclosure of information security breaches on covered entities' own initiatives. Rather, failure to disclose information security breaches could implicitly violate the *Model Code* in two ways: deceptively continuing to collect information despite knowledge of security breaches and failing to disclose information security breaches at a data subject's written request.

PIPEDA prohibits the collection of personal information "through deception," by "misleading or deceiving individuals about the purpose for which information is being collected."[177] At some point, covered entities have enough reason to suspect that the personal information they maintain could be exposed by security breach, and that failing to disclose that risk on an ongoing basis could be misleading to prospective data subjects. (Given that "purpose" implies an intentional aspect, however, it may be that covered entities do not mislead regarding the purpose of data use when they fail to disclose unintended security breaches.)

In addition, PIPEDA makes specific provision for entities to provide information to a data subject about "the existence, use and *disclosure of*

173. *Id.* at sched. 1, ¶ 4.2.4.

174. *Id.* at sched. 1, ¶ 4.5.

175. *Id.* at sched. 1, ¶¶ 4.7-4.7.5.

176. Privacy Commissioner of Canada, *PIPED Act Summary #137 Telecommunications Company Accused of Not Protecting Account Against Unauthorized Access*, <http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030306_6_e.asp> (Mar. 6, 2003). A husband broke into Internet records of his wife's cellular phone account, but because the husband had access to his wife's home and cellular phone account statement, the Commissioner concluded that the company could have done nothing more "to prevent a situation in which a husband impersonated a wife to gain access to her account." *Id.*

177. PIPEDA at sched. 1, ¶ 4.4.2.

his or her personal information" upon written request.[178] PIPEDA provides various exemptions for entities to refuse data subjects access to information about how their data has been disclosed or used.[179] Nonetheless, covered entities' failure to disclose information security breaches to data subjects that had requested such information could not be in meaningful compliance with this PIPEDA provision.

2. *Australian Privacy Act 1988*

The current form of *Australia's Privacy Act 1988* recognizes one of two substantive information practice standards:[180] approved codes, which are developed and enforced by private industry, but approved by the Australian Privacy Commissioner,[181] and the otherwise generally applicable *National Privacy Principles* (NPP).[182] As a practical matter, it does not appear that many private industry privacy codes have been approved, so the NPP governs most covered organizations.[183] The *Privacy Act 1988* covers a very broad definition of personal information – essentially any information regarding a person who can be readily identified.[184] In contract, the *Privacy Act 1988* only applies to a technical statutory definition of "organizations,"[185] which includes individuals, bodies corporate, partnerships, trusts or any other unincorporated association (but excluding "small business operators," registered political parties, agencies, Australian state or territorial authorities, or their instrumentalities.[186] The basic test for the small business operator exemption is whether the organization earns less than $3 million Australian, but the actual specifics of this exemption are substantially more involved.)[187]

178. *Id.* at § 8(1); *id.* at sched. 1, ¶ 4.9; *see also id.* at sched. 1, ¶¶ 4.9.1 to 4.9.6 (describing process of data subject access to data on data subject maintained by entity).

179. *Id.* at § 9.

180. Privacy Act, 1988, ch. 119, §§ 6A, 16A(1), (2) (Austl.), amended by Privacy Amendment (Private Sector) Act 2000, ch. 155 (Austl.) (available at <http://www.privacy.gov.au/publications/privacy88_240103.doc>).

181. *Id.* at §§ 18BA-18BI.

182. *Id.* at sched. 3.

183. *See* Office of the Federal Privacy Commissioner, *Privacy Codes*, <http://www.privacy.gov.au/business/codes/index.html> (accessed July 1, 2004) (listing only the Market and Social Research Privacy Code, the General Insurance Information Privacy Code and Clubs Queensland Industry Privacy Code as approved codes).

184. Privacy Act, 1988, c. 119, § 6(1) (defining personal information as "information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion").

185. *Id.* at § 16A(1), (2).

186. *Id.* at § 6C(1).

187. *See id.* at § 6D(1); *but see id.* at §§ 6D(4), (5), (6), 6DA, 6E, 6EA.

The *Privacy Act 1988* defines interferences with privacy as breaches of either approved codes or the *NPP* (if no approved code applies) in relation with the claimant.[188] Prior to judicial proceedings under the *Privacy Act 1988*, a claimant must take his complaint to the entity involved to attempt resolution.[189] Afterwards, the claimant may bring his complaint to either the Privacy Commissioner (in the absence of an approved code) or an ombudsman selected by an applicable approved code.[190] The Privacy Commissioner investigates the complaint and determines its validity.[191] After the investigation, the Privacy Commissioner provides a declaration that either dismisses the complaint or fixes an appropriate remedy (including money damages for emotional harm) for the *Privacy Act 1988* violation alleged in the complaint.[192] While the Commissioner's declaration is neither binding nor conclusive on either party,[193] organizations must comply with those portions of a Commissioner's declaration that order an organization to cease an activity or perform an act.[194] The claimant, the Privacy Commissioner, or the ombudsman (under the applicable approved code) may petition an Australian federal court or federal magistrate to enforce a determination by the Privacy Commissioner (or ombudsman, if applicable),[195] although the court hears the complaint *de novo*.[196]

The NPP requires organizations to disclose the purposes for which personal data are collected to data subjects at or prior to the time the data are collected.[197] Use or disclosure of data for purposes other than those disclosed to the data subject (secondary purposes) is largely prohibited.[198] (Major exceptions include: 1) when the new purpose is related to and reasonably anticipated by the data subject; 2) when the organization has the data subject's consent; 3) for public health purposes; 4) for law enforcement purposes; or 5) as otherwise reasonably required or authorized by law.)[199] In addition, organizations "must take reasonable steps to protect" personal information from "misuse and loss and from unauthorised access, modification or disclosure."[200] Like the DPA or

188. *Id.* at § 13A(1)(a), (b).
189. *Id.* at § 40(1A).
190. *Id.* at § 35(1), (1A), (1B).
191. *Id.* at §§ 40-47.
192. *Id.* at § 52(1), (1A), (2), (3).
193. *Id.* at § 52(1B).
194. *Id.* at § 55.
195. *Id.* at § 55A(1), (2).
196. *Id.* at § 55A(5).
197. *Id.* at sched. 3, ¶¶ 1.3, 1.5.
198. *Id.* at sched. 3, ¶ 2.1.
199. *Id.*
200. *Id.* at sched. 3, ¶ 4.1.

PIPEDA, the *Privacy Act 1988* does not contemplate entities disclosing unauthorized security breaches.

However, the *Privacy Act 1988* also requires organizations to make written notes of uses and disclosures for secondary purposes.[201] This provision also does not contemplate unintended, unauthorized disclosures, but may nonetheless require that organizations record when information security breaches affect data subjects. Consequently, that record may be required to be disclosed: 1) under provisions that require organizations to generally disclose what data it maintains, for what purposes, and how it discloses that data;[202] and 2) under provisions that generally require organizations to provide data subjects access to data pertaining to them.[203] The exceptions to requirements that data subjects have access to data maintained by organizations include situations that would pose a serious and imminent threat to the life or health of any individual, have an unreasonable impact upon the privacy of others, would be prejudicial in litigation or negotiation, or the access would be otherwise unlawful, or prejudicial to law enforcement.[204] Failing to disclose an information security breach after a data subject's request encompasses information about the disclosure of data pertaining to the data subject would seem to violate the *NPP* and the *Privacy Act 1988*.

3. *Canadian and Australian Common Law*

Ultimately, both Canadian and Australian laws require covered entities to make representations to data subjects about how their personal data are used and disclosed as those covered entities gather data. As with the American and British examples, these representations may dovetail with existing common law doctrines of fraud and negligent misrepresentation, even where no *per se* violation of PIPEDA or the *Privacy Act 1988* has occurred.

In the context of mandated representations about information security practices, businesses' knowing concealment of ongoing information security breaches would seem to constitute fraud under both Canadian and Australian common law. The exact contours of deceit and fraud in Australian and Canada are beyond the scope of this article. However, both jurisdictions naturally recognize fraud, and may extend liability to businesses which knowingly fail to disclose ongoing information security breaches as they collect data under the auspices of their represented information practices.

201. *Id.* at sched. 3, ¶ 2.2.

202. *Id.* at sched. 3, ¶ 5.2.

203. *Id.* at sched. 3, ¶ 6.1.

204. *Id.* at sched. 3, ¶ 6.1(a), (c), (e), (f), (i), (j), (k).

Likewise, the precise limits of negligent misrepresentation under Canadian and Australian common law are beyond the scope of this article. Still, we can observe that both Canada[205] and Australia[206] have adopted the doctrine of negligent misrepresentation articulated in *Hedley Byrne*. Albeit without further inquiry, it would seem that both of these Commonwealth jurisdictions would also hold liable businesses that negligently omitted discussion of security breaches while making representations about their information security practices to data subjects.

III. CONCLUSION

As can be seen, the scope of the duty to disclose breaches in an organization's information security extends far beyond even the maligned section 1798.82 of California's *Security Breach Information Act*. In this way, the complaints about section 1798.82 are unfounded: the California law does not impose a dramatically new obligation. Moreover, as businesses become increasingly global, privacy legislation becomes increasingly widespread. Many jurisdictions have laid the foundation for an obligation to disclose breaches of information practices.

In another way, the complaints about section 1798.82 reflect misgivings about a burgeoning duty to secure information. Some aspects of these misgivings are well-founded: the duty to disclose information security breaches does heighten the possibility of liability from security breaches and adds market discipline to the costs of security breaches. (One study found that publicly-traded firms which disclosed security breaches lost 2.1% of their market value within two days of the disclosure.)[207] Misgivings about section 1798.82, and duties to secure information and disclose security breaches, stem from a disgruntled

205. *See* Robert Hollyman, *Hercules Managements and the Duty of Care in Negligent Misstatement: How Dispensable is Reliance?*, 34 U. Brit. Colum. L. Rev. 515, 516 (2001) (citing *Hercules Managements Ltd. v. Ernst & Young*, 2 S.C.R. 165 (Can. 1997) (available at <http:// www.canlii.org/ca/cas/scc/1997/1997scc50.html>); *Queen v. Cognos, Inc.*, 1 S.C.R. 87 (Can. 1993) (available at <http://www.canlii.org/ca/cas/scc/1993/1993scc3.html>); *Haig v. Bamford*, 1 S.C.R. 466 (Can. 1997)).

206. *See* Adrian Baron, *The "Mystery" of Negligence and Economic Loss: When is a Duty of Care Owed?*, 19 Australian B. Rev. 1 (Feb. 14, 2000) (available at 2000 ABR LEXIS 4) (citing *Perre v. Apand* 73 ALJR 1190 (Austl. 1999) (available at <http://www.austlii.edu.au/au/cases/cth/high _ct/1999/36.html>); *Esanda Finance Corp. v. Peat Marwick Hungerfords* 188 CLR 241 (Austl. 1997) (available at <http://www.austlii.edu.au/au/cases/cth/high_ct/unrep305.html>)); *see also* Colin Phegan, *Reining in Foreseeability: Liability of Auditors to Third Parties for Negligent Misstatement (Esanda Finance Corporation Limited v. Peat Marwick Hungerfords (Reg) and Hercules Managements Ltd. v. Ernst and Young)*, 97 Tort L.J. 4 (1997).

207. Huseyin Cavusoglu et al., *The Effect of Internet Security Breach Announcements on Market Value of Breached Firms and Internet Security Developers* 2, <http://www.utdallas.edu/~huseyin/breach.pdf> (2002).

perception that collecting and maintaining data has become an increasingly risky proposition. Given the prevalence of computer intrusions and other kinds of information security breaches and the extensive obligations to ensure information security, the perception is increasingly correct. Data collectors can respond to that risk in at least three ways: they can expand the necessary resources to secure the information they collect, they can purchase the necessary insurance to guard against liability, or they can curtail their collection and maintenance of data.

Despite the high costs of insurance and added security and the low cost of expunging data, businesses are most likely to outright reject restricting their data collection as unacceptable. But restricting data collection is subject to the same cost-benefit analysis as insurance and adding security: business only reject restricting data collection outright because they do not really regard data collection as risky. But if data collectors must become reconciled to the growing risk in data collection because of potential liability, it is because data collection has always been risky for data subjects. As the review above shows, increasingly widespread legislation has begun to force data collectors to share that risk. Businesses will not seriously consider limiting the scope of their data collection until they understand and properly value the risks of data collection.